

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MAINE

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
BHADBABBY@ICLOUD.COM THAT IS  
STORED AT PREMISES CONTROLLED  
BY APPLE INC.

Case No. 2:21-mj-296-JHR

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Brian Rose, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with the account assigned BHADBABBY@ICLOUD.COM (hereinafter the Target Apple Account) that is stored at premises owned, maintained, controlled, or operated by Apple Inc. (“Apple”), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Detective with the Lewiston Maine Police Department and have been employed as a law enforcement officer with that department since 1999. I have been assigned as Task Force Officer with the Federal Bureau of Investigation since May 2021. In the course of

my law enforcement training and experience, I have had an opportunity to search for, seize, and personally observe what I have recognized to be and what was later confirmed by drug analysis to be scheduled drugs, including but not limited to heroin, fentanyl, cocaine, marijuana (both dried and growing), cocaine base, methamphetamine and various narcotics lawfully available only by prescription. As a result, I am personally familiar with the appearance of each of those substances. I have drafted a number of drug related search and arrest warrants and have assisted in the execution of numerous search and arrest warrants in which controlled substances, drug paraphernalia, and other contraband were found. Through my training and experience, I have become familiar with the habits, methods, routines, practices, and procedures commonly employed by persons engaged in the trafficking of illegal drugs.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 21, United States Code, Sections 841(a)(1) and 846 have been committed by Shawna Burch and others. There is also probable cause to search the information described in Attachment A for evidence of these crimes as described in Attachment B.

### **JURISDICTION**

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **PROBABLE CAUSE**

6. This application is being submitted contemporaneously with my application for a search warrant for information associated with Facebook User ID 100055713279926. My affidavit submitted in support of that warrant is attached hereto and incorporated herein as Exhibit 1. The information contained in Exhibit 1, combined with the additional facts below, demonstrate that Shawn Burch has engaged in the possession and distribution of methamphetamine, and that evidence of such offenses will be found information associated with the Target Apple Account.

7. A preservation request for information associated with the Target Account was sent to Apple on September 8, 2021.

### **BACKGROUND CONCERNING APPLE**<sup>1</sup>

8. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

9. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

---

<sup>1</sup> The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at [https://www.apple.com/business/docs/iOS\\_Security\\_Guide.pdf](https://www.apple.com/business/docs/iOS_Security_Guide.pdf), and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

- a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
- b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.
- c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple’s servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user’s Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.
- d. Game Center, Apple’s social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth, to determine a user’s approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

10. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

11. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

12. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

13. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is

linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

14. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user’s photos and videos, iMessages, Short Message Service (“SMS”) and Multimedia Messaging Service (“MMS”) messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user’s instant messages on iCloud Drive. Some of this data is stored on Apple’s servers in an encrypted form but can nonetheless be decrypted by Apple.

15. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to controlled substance trafficking, may be found in the files and records described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element and to identify conspirators and accomplices.

16. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of controlled substance trafficking, including to communicate and facilitate controlled substance trafficking. Specifically, as detailed in Exhibit 1, I am aware of specific evidence that Burch has previously engaged in electronic communications regarding controlled substance transactions by means of an Apple Device, and that these communications included both text and photos. Further, there is evidence that at least one of Burch’s one of controlled substance supplier’s telephone number will be found in the iCloud account identified in Attachment A.

17. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device



identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

18. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

19. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. I am aware that individuals involved in controlled substance trafficking often employ social media and messaging applications which can be downloaded to a mobile device or cell phone. As detailed in Exhibit 1, Burch utilized Facebook messaging to communicate with others regarding drug transactions. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

20. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

21. Based on the forgoing, I request that the Court issue the proposed search warrant.

22. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.



Task Force Officer Brian Rose  
Federal Bureau of Investigation

Sworn to telephonically and signed  
electronically in accordance with the  
requirements of Rule 4.1 of the Federal Rules  
of Criminal Procedure

Date: Nov 10 2021

City and state: Portland, ME



*Judge's signature*  
\_\_\_\_\_  
John H. Rich III, U.S. Magistrate Judge

*Printed name and title*